# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/002963

International filing date: 17 February 2005 (17.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-057629
Filing date: 02 March 2004 (02.03.2004)

Date of receipt at the International Bureau: 07 April 2005 (07.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/JP2005/002963

17.02.2005

# 日本国特許庁
# JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

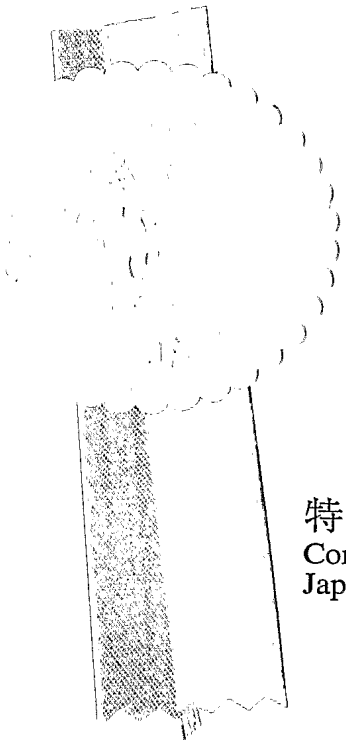
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　３月　２日

出願番号
Application Number: 特願２００４－０５７６２９

[ST. 10/C]: ［ＪＰ２００４－０５７６２９］

出願人
Applicant(s): 露崎　典平



２００５年　３月２５日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３０２６７７０

【書類名】　特許願
【整理番号】　Q00953X0
【あて先】　特許庁長官殿
【国際特許分類】　E05B 49/00
【発明者】
　【住所又は居所】　千葉県茂原市早野１８２０
　【氏名】　露崎　典平
【特許出願人】
　【識別番号】　595122268
　【氏名又は名称】　露崎　典平
【代理人】
　【識別番号】　100064447
　【弁理士】
　【氏名又は名称】　岡部　正夫
【選任した代理人】
　【識別番号】　100085176
　【弁理士】
　【氏名又は名称】　加藤　伸晃
【選任した代理人】
　【識別番号】　100106703
　【弁理士】
　【氏名又は名称】　産形　和央
【選任した代理人】
　【識別番号】　100096943
　【弁理士】
　【氏名又は名称】　臼井　伸一
【選任した代理人】
　【識別番号】　100091889
　【弁理士】
　【氏名又は名称】　藤野　育男
【選任した代理人】
　【識別番号】　100101498
　【弁理士】
　【氏名又は名称】　越智　隆夫
【選任した代理人】
　【識別番号】　100096688
　【弁理士】
　【氏名又は名称】　本宮　照久
【選任した代理人】
　【識別番号】　100102808
　【弁理士】
　【氏名又は名称】　高梨　憲通
【選任した代理人】
　【識別番号】　100104352
　【弁理士】
　【氏名又は名称】　朝日　伸光
【選任した代理人】
　【識別番号】　100107401
　【弁理士】
　【氏名又は名称】　高橋　誠一郎

【選任した代理人】
　【識別番号】　100106183
　【弁理士】
　【氏名又は名称】　吉澤　弘司
【選任した代理人】
　【識別番号】　100120064
　【弁理士】
　【氏名又は名称】　松井　孝夫
【手数料の表示】
　【予納台帳番号】　013284
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
本体と相手側とのペアによって構成される認証装置であって、該本体、或は相手側、或は本体と相手側の双方に、自発的にランダムパルスを発生するランダムパルス発生器（以下RPGと呼ぶ）と、このＲＰＧが生成するランダムパルスに基づき認証信号を出力する手段と、認証信号を記憶する手段と、認証信号を送信／受信する通信手段と、認証信号の通信制御及び照合等を行う制御手段から成る認証装置。
【請求項２】
前記制御手段は、ペアを構成する相手側に設けた記憶手段に記憶された認証信号を受信し、受信した認証データを本体に設けた記憶手段の認証データと照合し、その照合結果に従って相手側の認証を行う、また認証の終了後、認証データを更新し、更新された新たな認証データを本体及び相手側の記憶手段に書き込むことを特徴とする請求項１に記載の認証装置。
【請求項３】
更に、制御手段の照合結果に従い駆動装置を制御する駆動装置制御手段を有する、請求項１または２に記載の認証装置。
【請求項４】
前記本体は、電子錠の本体であり、前記相手側は、ICカードを含む鍵であることを特徴とする、請求項１または２に記載の認証装置。
【請求項５】
前記ＲＰＧは、原子核の崩壊で放出されるα粒子、ベータ線またはガンマ線を検出してランダムパルスを発生することを特徴とする請求項１乃至４のいずれか記載の認証装置。
【請求項６】
α粒子放出体に$^{241}$Am、$^{210}$Pb-$^{210}$Po、$^{210}$Po、$^{244}$Cm等を、ベータ線放出体に210Pb等を使用することを特徴とする請求項５に記載の認証装置。
【請求項７】
前記RPGは、熱電子、ノイズあるいはジッター等を検出してランダムパルスを発生させることを特徴とする請求項１乃至４のいずれかに記載の認証装置。
【請求項８】
前記通信手段は、認証データの送受を赤外線通信あるいは無線通信で行うことを特徴とする請求項１乃至７のいずれかに記載の認証装置。
【請求項９】
前記通信手段は、接触による回路接続により、認証データの送受信を行うことを特徴とする請求項１乃至７のいずれかに記載の認証装置。
【請求項１０】
本体、或は相手側、或は本体と相手側の双方に設けたランダムパルス発生器（以下RPGと呼ぶ）によって自発的にランダムパルスを発生するステップと、このＲＰＧが生成するランダムパルスに基づき認証信号を出力するステップと、認証信号を記憶するステップと、認証信号を送信／受信するステップと、認証信号の通信制御及び照合等を行う制御ステップから成る認証方法。
【請求項１１】
前記制御ステップは、ペアを構成する相手側に設けた記憶手段に記憶された認証信号を受信し、受信した認証データを本体に設けた記憶手段の認証データと照合し、その照合結果に従って相手側の認証を行う、また認証の終了後、認証データを更新し、更新された新たな認証データを本体及び相手側の記憶手段に書き込むことを特徴とする請求項１０に記載の認証方法。
【請求項１２】
更に、制御手段の照合結果に従い駆動装置を制御する駆動装置制御ステップを有する、請求項１０または１１に記載の認証方法。
【請求項１３】

前記ＲＰＧは、原子核の崩壊で放出されるα粒子、ベータ線またはガンマ線を検出してランダムパルスを発生することを特徴とする請求項１０乃至１２のいずれか記載の認証方法。

【請求項１４】

α粒子放出体に$^{241}$Am、$^{210}$Pb-$^{210}$Po、$^{210}$Po、$^{244}$Cm等を、ベータ線放出体に210Pb等を使用することを特徴とする請求項１３に記載の認証方法。

【請求項１５】

前記RPGは、熱電子、ノイズあるいはジッター等を検出してランダムパルスを発生させることを特徴とする請求項１０乃至１２のいずれかに記載の認証方法。

【請求項１６】

前記通信ステップは、認証データの送受を赤外線通信あるいは無線通信で行うことを特徴とする請求項１０乃至１５のいずれかに記載の認証方法。

【請求項１７】

前記通信ステップは、接触による回路接続により、認証データの送受信を行うことを特徴とする請求項１乃至１５のいずれかに記載の認証方法。

【書類名】明細書
【発明の名称】ランダムパルス発生器（RPG）を使用した認証装置及び認証方法
【技術分野】
【０００１】
本発明は完全なランダムパルスを自発的に発生するランダムパルス発生器を使用して、完全ランダムな信号を認証信号として使用する認証装置及び認証方法に関するものである。
【背景技術】
【０００２】
従来の認証装置、例えば電子錠は、鍵メーカーが認証用データをあらかじめ決め、鍵本体（錠）と本体に差し込む鍵とを組として完成させ販売し、使用者は完成品を購入して玄関ドアなど必要な個所に取り付けて使用していた。また電子錠の他のタイプとしては、鍵をかけた時刻を認証データとして鍵本体と鍵とに記憶させ、開錠の際に記憶した認証データを照合するもの（特開平７―２３３６６３）、認証データとして声紋を利用したもの（例えば特開平８－２５７２１６）等があった。
【特許文献１】特開平７－２３３６６３号公報
【特許文献２】特開平８－２５７２１６号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
従来の認証装置を、その具体的な適用例である電子錠について考察する。従来の電子錠のうち、メーカーが認証用データを予め決めて製造されたものは、認証用のデータが固定されて自由に変更することが出来ないか（実際は、メーカーがプログラムで認証用データを作成しており、その組み合わせ数に制限があり、同一の認証データが使用される危険があった）、又は、変更が可能なタイプでもテンキーなどの入力であり、使用する桁数や組み合わせが制限されていた。
【０００４】
また、多くの場合、メーカーは製造した認証用のデータを保守・サービスのために保存する必要があり、その際に、機密の保持のために膨大な費用をかけていた。例えば、メーカーは、鍵の組み合わせに制限があると、同一認証データが使用される危険が増大するため、同じ組の鍵が同一地域に配布されないよう管理する必要があった。更に、データの漏洩防止は管理者の資質に依存しなければならず、完全な防止対策におのずと限界があった。
なお、同じ認証用のデータが使用されると、電子錠を使用した車などでは同じ駐車場に駐車していた別の車のドアが反応して開く等の不都合が生じる。
【０００５】
認証用データとして施錠時の時刻を利用するものであっても、時刻は経時的に順次変化するデータであるから、不規則性を要件とする認証データとしては不適当である。例えば、データの桁数によっては容易に解読されてしまうし、また、同時使用により鍵のコピーが容易に作成されてしまうなどの不都合があり、セキュリティの面で問題があった。
また声紋を利用するタイプのものは、声紋の判定のための装置が複雑となり一般向けの電子錠としては不向きであった。
【０００６】
なお、時刻にしても、声紋にしても、いずれも、外部環境に依存するもの（即ち、鍵または鍵本体内で、いかなる環境にも左右されない認証信号を生成することは不可能）であるから、例えばその仕組みを知った人間による人為的な操作より開錠することは可能であって、セキュリティの面で限界があった。
【課題を解決するための手段】
【０００７】
本願発明は、上述した従来の認証装置、特に電子錠における問題点を解消するために創

作されたもので、本体と相手側とのペアによって構成される認証装置であって、該本体、或は相手側、或は本体と相手側の双方に、自発的にランダムパルスを発生するランダムパルス発生器（以下RPGと呼ぶ）と、このＲＰＧが生成するランダムパルスに基づき認証信号を出力する手段と、認証信号を記憶する手段と、認証信号を送信／受信する通信手段と、認証信号の通信制御及び照合等を行う制御手段から成る認証装置を提供する。

【０００８】

また、本願発明は、該本体、或は相手側、或は本体と相手側の双方に設けたランダムパルス発生器（以下RPGと呼ぶ）によって自発的にランダムパルスを発生するステップと、このＲＰＧが生成するランダムパルスに基づき認証信号を出力するステップと、認証信号を記憶するステップと、認証信号を送信／受信するステップと、認証信号の通信制御及び照合等を行う制御ステップから成る認証方法を提供する。

【発明の効果】

【０００９】

本発明に係る認証装置及び認証方法は、例えば、自然崩壊で無限に放出されるα粒子を利用したRPGを鍵本体内部に組み込み、RPGから、環境条件に全く作用されずかつ人的コントロールが一切出来ないオリジナルでランダムな信号を得て、この信号を鍵の認証信号として使用するので、鍵自身においていつでも認証信号の生成が可能で、使用のたびに新しい完全にランダムなデータを書込むことができ、コピー不能とし、そのため、鍵メーカーでのデータ管理が不要で、使用者側で完全なセキュリティを確保でき、安全性が確立出来る等の優れた効果がある。

【発明を実施するための最良の形態】

【００１０】

以下、図面を参照し、本発明のランダムパルス発生器（RPG）を使用した認証装置／方法を、電子錠を実施例として詳細に説明する。

図１Aは、本願発明にかかる電子錠の概要を説明する図であり、図１Bは図１Aの電子錠の使用状態を説明する図である。図において、１はドアノブ、２は指紋認証装置、３はテンキー、１０は電子錠本体、１１は電子錠本体に組み込まれたランダムパルス発生器（以下ＲＰＧという）、１２は同じく電子錠本体に組み込まれたメモリ、２０は鍵、２１は鍵に組み込まれたメモリを示す。

【００１１】

完全なランダムパルスを発生させるRPGは、本発明者が既に特許権者となっている特許第2926539号に記載されているα粒子検出装置を使用する。α粒子放出体は自然崩壊する$^{241}$Am、$^{244}$Cm、$^{210}$Pb-$^{210}$Po、$^{210}$Po等を使用する。金庫のように遮蔽設置スペースがある部位に使用する電子錠であればベータ線やガンマ線を使用しランダムパルスを発生するRPGでも良い。

α粒子やベータ線、ガンマ線は、温度,圧力、湿度や電磁波など環境に影響されない為、人的制御が出来ない。この特質は他の方法では実現出来ない安全が確保できる重要な要素である。完全な安全性が要求されない部位に使用する電子錠であれば熱電子や半導体のジッターなどをランダムパルスの発生源とするRPGでも良い。

【００１２】

鍵本体には、RPGとRPGから送出されるランダムパルスを認証信号として使用できるようにするための電子回路、認証信号を記憶するための回路（記憶素子）、通信の形態に応じた認証信号を送受するための回路、必要に応じ、アンテナ及び通信素子及び電源などが組み込まれる。なお、電源は外部から通信（電磁誘導、電波や端子接続）で供給する方法もある。

まず自発的にランダムパルスを発生するランダムパルス発生器（RPG）１１について説明する。

【００１３】

RPGは、図2に示すようにパルス発生部１１Ａ、プリアンプ部１１Ｂ、メインアンプ部１１Ｃ、波形成型部１１Ｄから構成されている。

パルス発生部１１Ａは鍵(電子錠)が要求される安全度に応じて素子を選択する。最も安全性が要求される鍵については、図３に示すようなα粒子放射体が取り付けられた素子(α放射体付きダイオード)を使用する。図示において、１１ｂはキャンシールを示す。α放射体から放出されるα粒子（He原子）の放出は温度、圧力、電磁波など環境に全く影響されず、電源も不要で自発的に半減期に応じて半永久的に放出される。つまりこの方式では認証に使用する原信号は人的制御が全く出来ない信号源を使用することが出来る事が特徴である。よって外部からは一切変更が出来ない信号発生源となる。なお、放射性カプセルの使用は、前述の特許第2926539号に開示がある。

【００１４】

鍵取り付け部位が完全な安全性を要求されない場合はパルス発生部を図４のようなダイオード（ツエナーダイオード）としても良い。

【００１５】

プリアンプ部１１Ｂは、パルス発生部１１Ａで生成された微小パルス信号をメインアンプ部１１Ｃの入力信号にするための増幅を行う。

メインアンプ部１１Ｃはノイズと明確に区別する為の増幅を行う。この回路でノイズ部が含まれる0.5V以下をノイズ信号が含まれる帯域としてディスクリーとする。デスクリートする電圧は要求される信号強度及びノイズレベルに応じて設定すればよい。（図５参照）

波形整形部１１Ｄは、メインアンプ部１１Ｃから先頭波形で出力されるパルスを、認証信号として取扱得るようパルス幅を加える。ＲＰＧから出力されるパルス波形を図５に示す。

【００１６】

なお、RPGからの信号を数値化して記憶する方法としては、図９に示したように、RPGのランダムパルスは、波高値とパルス間隔がランダムであるので、波高値の電圧をデジタル変換して乱数値とすることもできる。パルスの間隔がランダムであるのでパルス間隔を計測するクロックパルス数を乱数値とする事も出来る。また同図に示すように(電圧、クロックパルス数)の組み合わせとして用いることも出来る。例えば、パルス１は（９，５）、パルス２は（４，３）、パルス３は（７，６）、パルス4は（１０，３）等である。

【００１７】

鍵本体の回路を図６に示す。鍵本体１０は、電源モジュール１３、差込検知モジュール１４、トランシーバーモジュール１５、RPGモジュール１６から構成されている。

電源モジュール１３は、構成回路全体に動作電源を供給し、図示実施例では、５Ｖの安定化された電圧を供給するＤＣ－ＤＣコンバータＵ１が使用されている。

差し込み検知モジュール１４は、相手側となる鍵が差し込まれたのを、例えば鍵本体と鍵との接触により検知し（スイッチＳＷ２のＯＮ）、バッファ・ゲートＵ７を介し、ＲＰＧモジュールに起動信号を送る。

【００１８】

トランシーバーモジュール１５は、差し込まれた鍵との間で赤外通通信により信号を送受するモジュールである。Ｕ２は赤外線通信モジュールで、図示実施例で使用されているものは、赤外線発光ＬＥＤ，フォトダイオード、波形整形ＬＳＩをパッケージ化してある。Ｕ３Ａは単安定マルチバイブレータで、赤外線通信モジュールの出力パルス信号をトリガ入力し、その出力パルス信号を、RPGモジュールＵ６に送る。なお、Ｕ４はＡＮＤ回路、Ｕ５はインバータ回路で、赤外線通信モジュールの送受信信号の干渉を防いでいる。なお、トランシーバーモジュールは、赤外線通信以外の、光、電波等による無線通信を利用したものであってもかまわない。

図示実施例では、認証データの送受信を、トランシーバーモジュールを使用したものが例示されているが、本願発明はこれに限定されず、通信手段（認証信号の送受手段）は、接触による回路接続であってもよい。

【００１９】

RPGモジュール１６は通信の手順、信号の送出、信号の受信、及びデータの保管をする

とともに、信号発生源であるRPGを組み込んである。ＲＰＧモジュールは、また、鍵本体と鍵との認証データが同一であると判別されたときに、電子錠を開錠するための開錠出力を出力する。電子錠の開錠には、公知の手段が使用され、例えば、電磁式のロック機構を持つものであれば、これを制御する手段に制御信号を送り解除を指令する。鍵本体と鍵との通信手順については後述する。

【００２０】

図１０にRPGモジュールの構成例を示す。このモジュールは、ランダムパルス発生器１６Ａ、A/D変換回路１６Ｂ、基準電圧発生回路１６Ｃ、クロックパルス発生回路１６Ｄ、パルスカウンタ１６Ｅ、入出力端子(入出力回路)１６Ｆ、演算回路（演算・処理・制御回路）１６Ｇ、記憶回路１６Ｈ、表示・動作音出力回路１６Ｉ、鍵動作出力回路１６Ｊから構成される。演算回路１６Ｇは、入出力端子１６Ｆから入力される認証信号を、記憶回路１６に記憶した認証信号と一致するか判定する。判定結果は、表示・動作音出力回路１６Ｉに表示され、また、必要に応じ、外部に設けたスピーカから音声で知らせる。一致したときは、鍵動作出力回路を介して開錠出力を出力する。

【００２１】

ランダムパルス発生器１６Ａから出力されるパルスの間隔はランダムであるので、クロックパルス発生回路１６Ｄとパルスカウンタ１６Ｅを用いて、パルス間隔を計測し、そこで得たクロックパルス数を認証信号（認証データ）として利用する。あるいは、ランダムパルス発生器１６Ａから出力されるパルスの波高値とパルス間隔はランダムであるので、A/D変換回路１６Ｂと基準電圧発生回路１６Ｃを用いて、波高値の電圧をデジタル変換して認証信号（認証データ）として利用することもできる。図示実施例では、いずれの方法でも、あるいは両方を用いて認証信号を得ることができるように構成してあるが、いずれか一方のみの構成であってもかまわない。

なお、鍵の登録の際には、前述の手段で得た認証データを、記憶回路１６Ｈに記憶し、同時に、入出力端子１６Ｆから、鍵本体側のトランシーバーモジュール１５に送る。トランシーバーモジュールは、認証データを鍵側に送り、鍵側のトランシーバーモジュール２３を介して動作・記憶モジュール２４に記憶される。

【００２２】

RPGモジュール１６の構成は、図示のものに限定されず、鍵が取り付けられるセキュリティレベルに応じて、内部クロックや判定回路などを構成できるPICやCPUを持つ素子で置き換えることも出来る。ASICにしてワンチップ化することも可能である。

【００２３】

鍵本体に挿入する鍵には、認証信号を記憶するための回路と記憶素子、通信の形態に応じた認証信号を送受するための回路、必要に応じ、アンテナ及び通信素子及び電源などが組み込まれる。なお、電源は外部から通信（電磁誘導、電波や端子接続）で供給する方法もある。

【００２４】

鍵本体とペアとなる鍵の回路構成を図７に示す。鍵の構成は、電源モジュール２２、トランシーバーモジュール２３、動作・記憶モジュール２４から構成される。なお、鍵は、例えばＩＣカードのような形状、構造であってもかまわない。

電源モジュール２２は、構成回路全体に動作電源を供給し、図示実施例では、５Ｖの安定化された電圧を供給するＤＣ－ＤＣコンバータＵ１が使用されている。本実施例における電源モジュール２２は電池の挿入とともに信号電源が供給される構造となっているが、スイッチを押した時に信号の通信が開始するようにスイッチを組み込むことも可能である。

トランシーバーモジュール２３は、鍵本体との間で赤外通通信により信号を送受するモジュールである。その構成は、鍵本体のトランシーバーモジュール１５と同様である。ただし、ワンショット・マルチバイブレータＵ３Ａの出力は、動作・記憶モジュール２４の非同期受信ポートに送られる。

動作・記憶モジュール２４は汎用のＰＩＣ（周辺機器接続制御用ＩＣ）であって、演算

機能部、メモリ、入出力部等を有し、認証用データを記憶し、鍵本体と鍵との通信、認証データの照合等を制御するプログラムを内蔵する。図示実施例のものは、他に、タイマー、汎用通信ポート等も備えている。

【００２５】

次に、鍵本体と鍵との認証手順は、まず認証の相手側としての鍵の登録を行う。鍵の登録は、鍵に差し込めば自動的に認証し、相手側としての登録も可能であるが、取り付けられている装置や部位の安全性のレベルに応じて、図１Ａに示すような指紋認証装置２やテンキー３（暗証番号の入力）などと組み合わせる事もできる。

鍵の登録は、鍵を電子錠本体に差し込み、この鍵にＲＰＧからの信号を書き込み、同時に鍵本体に記憶する。

【００２６】

使用時の認証は、鍵本体に登録された鍵が差し込まれた時、差込側の鍵から送られてくる認証データが、本体に保存しておいた認証データと一致するか比較する。一致したら開錠する。開錠したらそのデータを削除し、同時に新しい認証データを双方に書き込む。この認証手順と認証データ保存は鍵を使用するたびに行われる。

【００２７】

鍵本体と相手側である鍵との間での通信手順の詳細を図8に示す。

(i)　鍵本体側は、差込検知トリガーモジュールが鍵の挿入を検知するとI(inquire)↓の文字キー（Ｉコマンド）を相手側である鍵側に送り、照合データの送信を要求する。

(ii)　鍵側は、鍵本体側からIコマンドを受信すると、保存していた照合データを”R○○・・・○↓”の文字列（コマンド）で鍵本体側に送信する（○・・・○は、RPGのデータにより変化する）。

(iii)　鍵本体側は、鍵側から照合データを受信すると、本体側で持っていたデータと比較し、不一致であるならばNG音を鳴らして認証を終了する。

(iv)　(iii)において、もし一致しているならば、ＲＰＧモジュールから開錠出力を適宜の駆動制御回路に送り、電子錠を開錠する。このとき、同時にRPGモジュールは認証データ（１００μsec程度のインターバルデータ）を更新し、新しい認証データとして鍵側に”W○・・・○↓”コマンドで送信する。

(v)　Wコマンドを受信すると、鍵側は、その新しいデータを次回の照合のために保存する。

(vi)　鍵本体側は、Wコマンドで送った認証データが正しく鍵側に受け取られたかどうかを確認するために、再度Iコマンドを鍵側に送信する。

(vii)　鍵側は、Iコマンドに応答して新しい認証データをRコマンドに付随して鍵本体側に返信する。

(viii)　鍵本体側は、受信した認証データを照合し、一致しているならば成功と判断しOK音を鳴らす。

(ix)　(viii)において、もし不一致ならば、再度データをWコマンドで鍵側に送信する。以降(v)乃至(viii)までを何回か繰り返し、それでも失敗した場合はFatal Error音を鳴らして認証を終える。

【００２８】

Fatal Errorとなった場合は、鍵本体及び鍵双方の保持している認証データが異なったままであるため、このままでは永久に使用できなくなる。これを回避するためには、本願発明では、以下の手順で初期化を実行し強制的に双方が同じデータを保持することができるようにしている。

(i)　RPGモジュールの２０ピンをGNDに短絡させる。

(ii)　鍵をレバースイッチ（差し込み検知トリガーモジュール）に入れる。

(iii)　OK音が鳴れば初期化成功

上記手順は、この方法は、例示であって、これら以外でも初期化は可能であり、安全性が確保できるような方法の選択が重要である。

【００２９】

以上、本願発明を、ＲＰＧを電子錠本体に組み込んだ例を示し説明したが、本願発明はこれに限定されずICタグなどに応用できる。ＲＰＧは、本体、相手側のいずれか、あるいは双方に組み込むことが可能である。また、本体と相手側との通信手順及び認証手順についても、ＲＰＧ，メモリ及び通信・認証の制御装置の配置によって変更可能であることは言うまでもない。

【図面の簡単な説明】

【００３０】

【図１Ａ】本発明の一実施例に係るランダムパルス発生器（ＲＰＧ）を使用した鍵の認証装置を示す説明図である。

【図１Ｂ】図１Ａに示す認証装置の使用状態の説明図である。

【図２】本発明にかかる実施例に使用されるランダムパルス発生器ブロック図である。

【図３】本発明に係るランダムパルス発生器に使用するα放射体付ダイオードを示す正面図である。

【図４】本発明に係るランダムパルス発生器に使用するツェナーダイオードを示す斜視図である。

【図５】本発明に係るランダムパルス発生器の出力波形を示すグラフである。

【図６】本発明に係る鍵本体の側の回路図例を示すブロック図である。

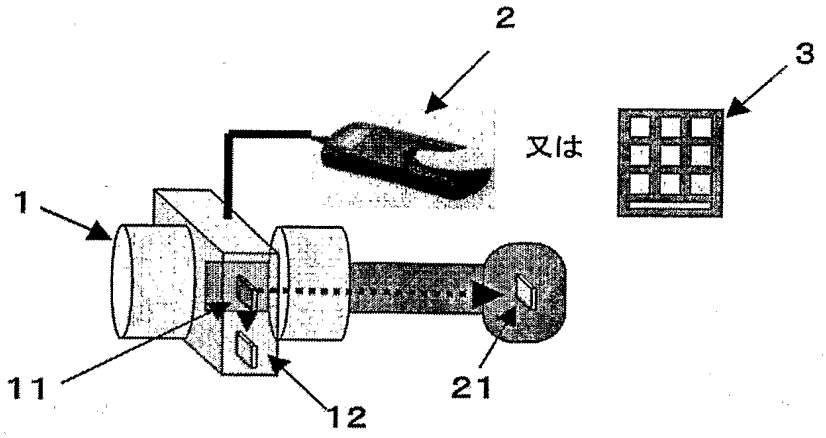
【図７】本発明に係る鍵側の回路例を示すブロック図である。

【図８】本発明に係る鍵本体とペアとなる鍵間の通信手順を示すフローチャートである。

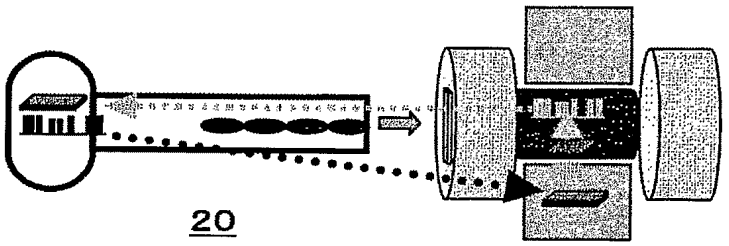
【図９】本発明に係るランダムパルス発生器の出力パルスの分類表示の方法を示す説明図である。

【図１０】本発明に係るRPGモジュールの構成例を示すブロック図である。

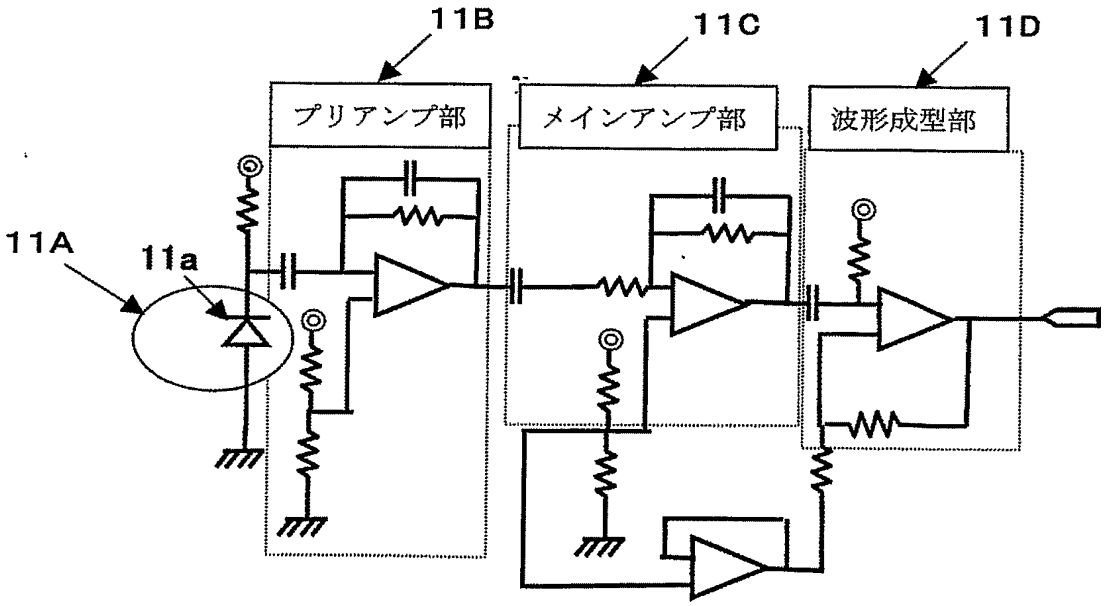
【書類名】図面
【図１Ａ】



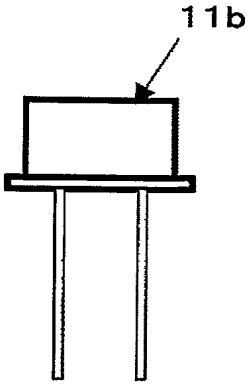

【図１Ｂ】




【図２】

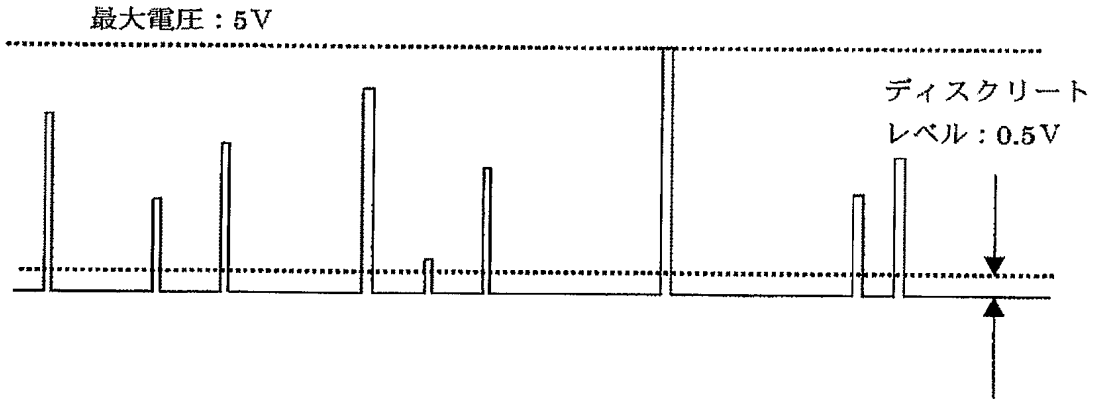


【図３】

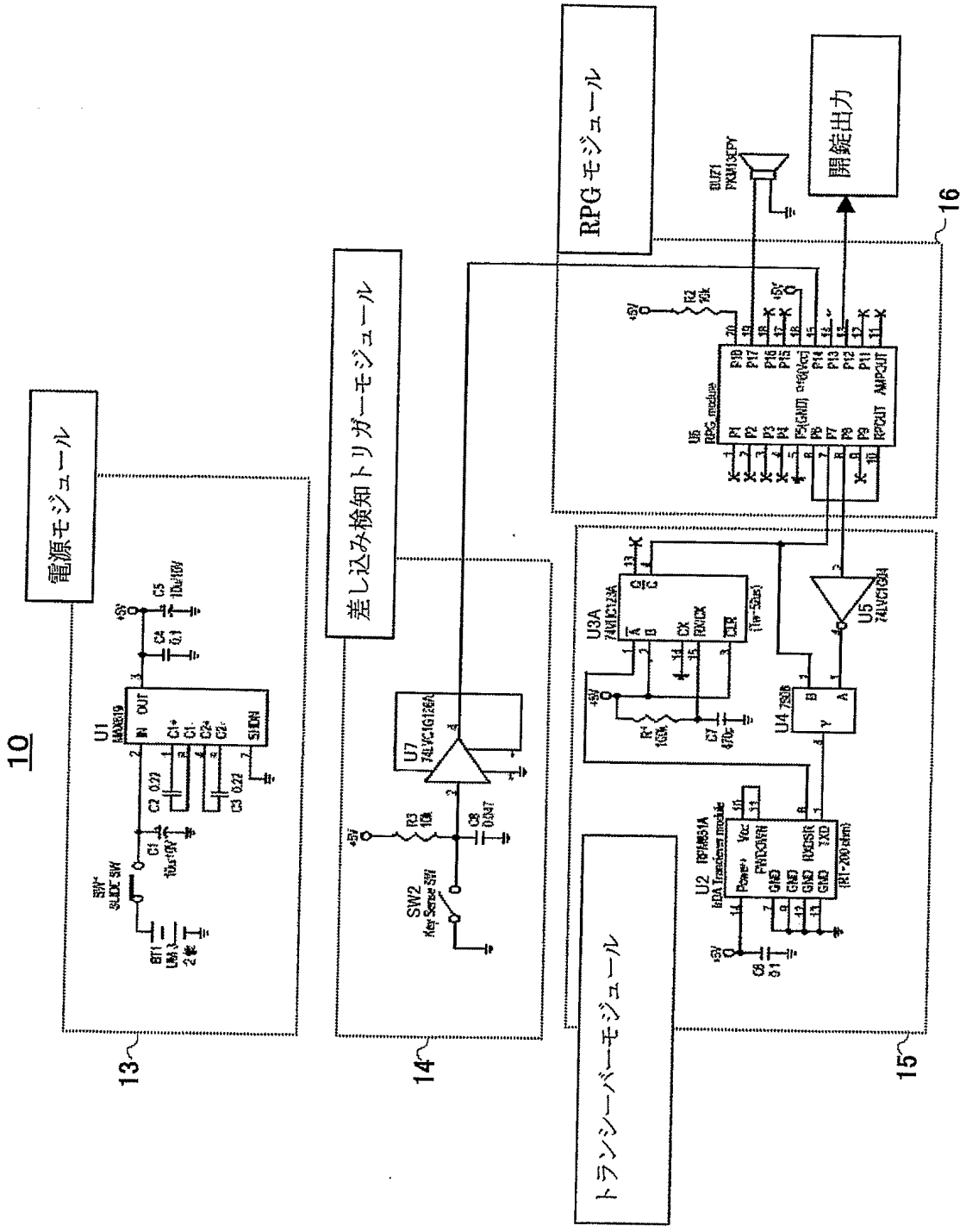



【図４】

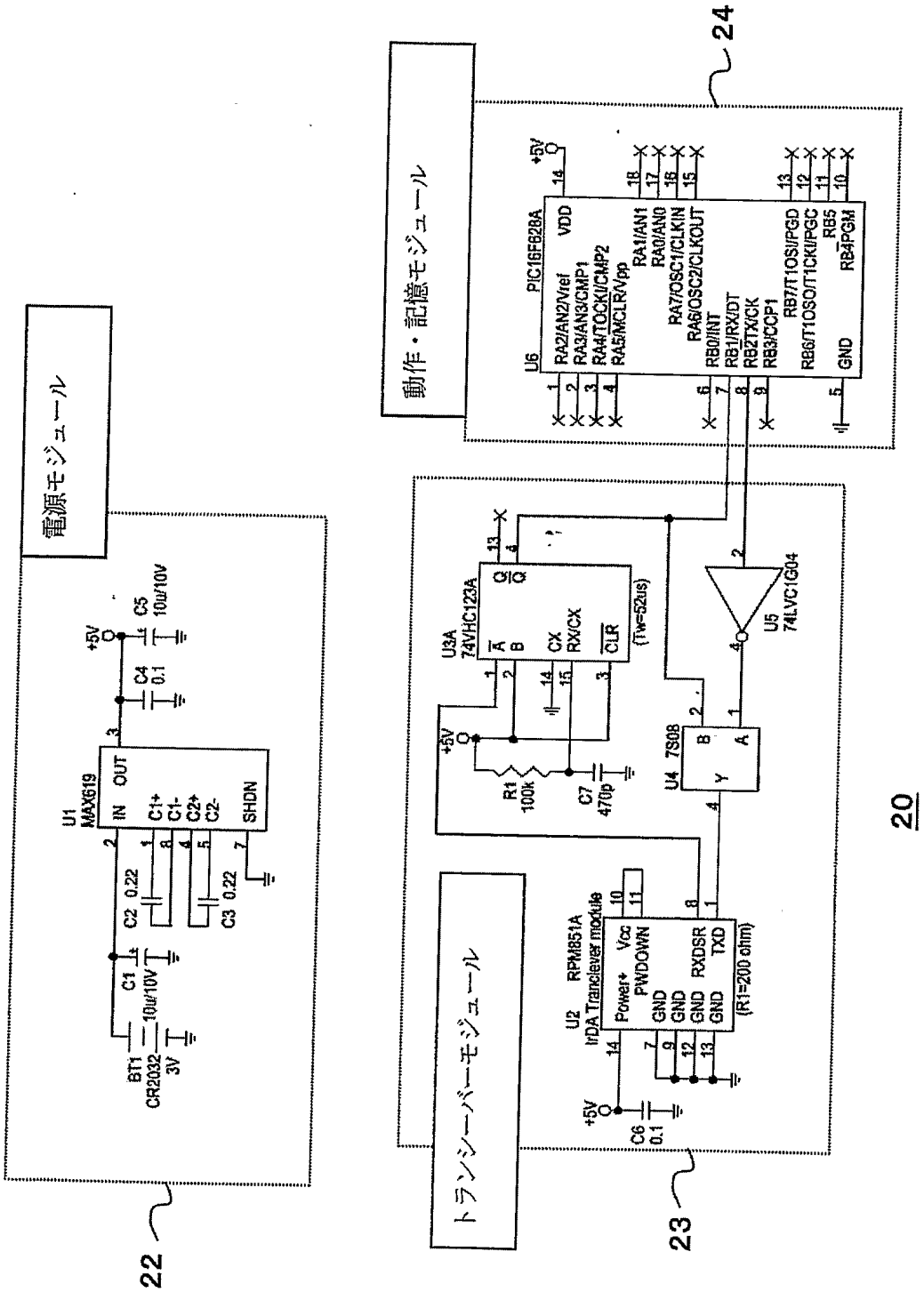
【図５】



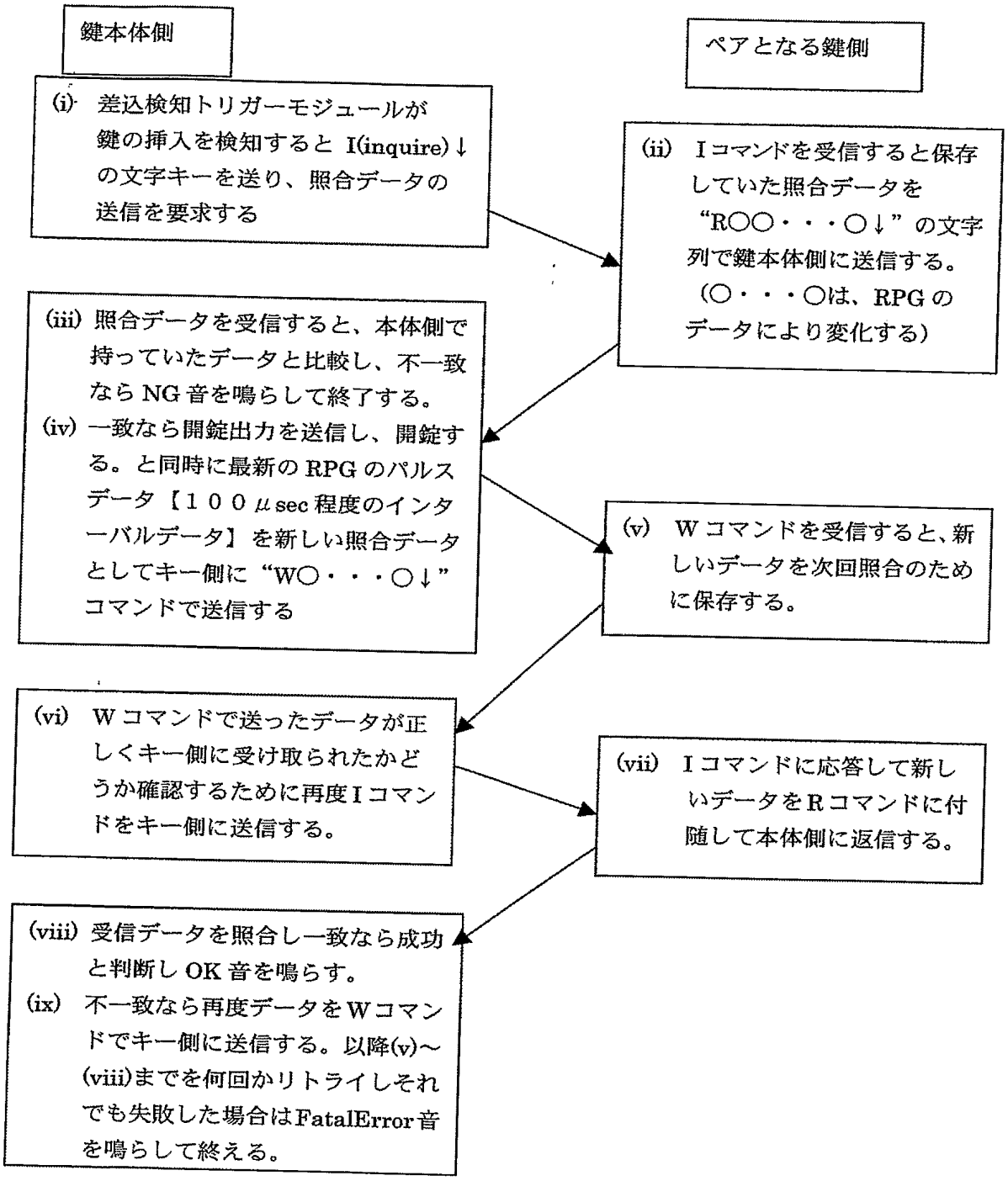
【図６】


電源モジュール
差し込み検知トリガーモジュール
RPGモジュール
開錠出力
トランシーバーモジュール
10
13
14
15
16
U1
MAX619
U7
74LVC1G126A
U3A
74VHC123A
U5
74LVC1G04
U4
7S08
U2
RPM951A
RPG_module
BUZ1
PKM13EPY
SW1
SLIDE SW
SW2
Key Sense SW
BT1
+5V
R1
100k
R2
10k
R3
10k
C1
10u/16V
C2
0.22
C3
0.22
C4
0.1
C5
10u/16V
C6
0.1
C7
470p
C8
0.047
R4
100k
P10
P17
P16
P15
P14
P13
P12
P11
P1
P2
P3
P4
P5(GND)
P6
P7
P8
P9
RPGOUT
AMPOUT
Vcc
GND
RXD5IR
TXD

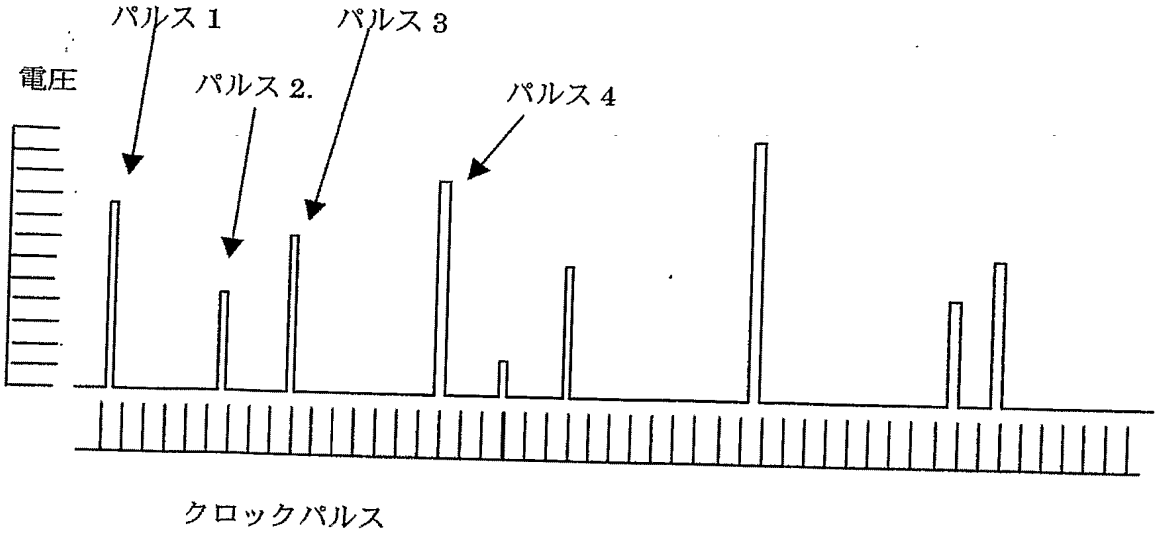
【図７】


電源モジュール
動作・記憶モジュール
トランシーバーモジュール
22
23
24
20
U1 MAX619
U2 RPM851A IrDA Tranciever module
U3A 74VHC123A
U4 7S08
U5 74LVC1G04
U6 PIC16F628A
BT1 CR2032 3V
C1 10uF/10V
C2 0.22
C3 0.22
C4 0.1
C5 10u/10V
C6 0.1
C7 470p
R1 100k
+5V
IN OUT C1+ C1- C2+ C2- SHDN
Power+ Vcc PWDOWN GND GND GND GND RXDSR TXD
(R1=200 ohm)
(Tw=52us)
RA2/AN2/Vref RA3/AN3/CMP1 RA4/T0CKI/CMP2 RA5/MCLR/Vpp
RA1/AN1 RA0/AN0 RA7/OSC1/CLKIN RA6/OSC2/CLKOUT
RB0/INT RB1/RX/DT RB2/TX/CK RB3/CCP1
RB7/T1OSI/PGD RB6/T1OSO/T1CKI/PGC RB5 RB4/PGM
VDD GND

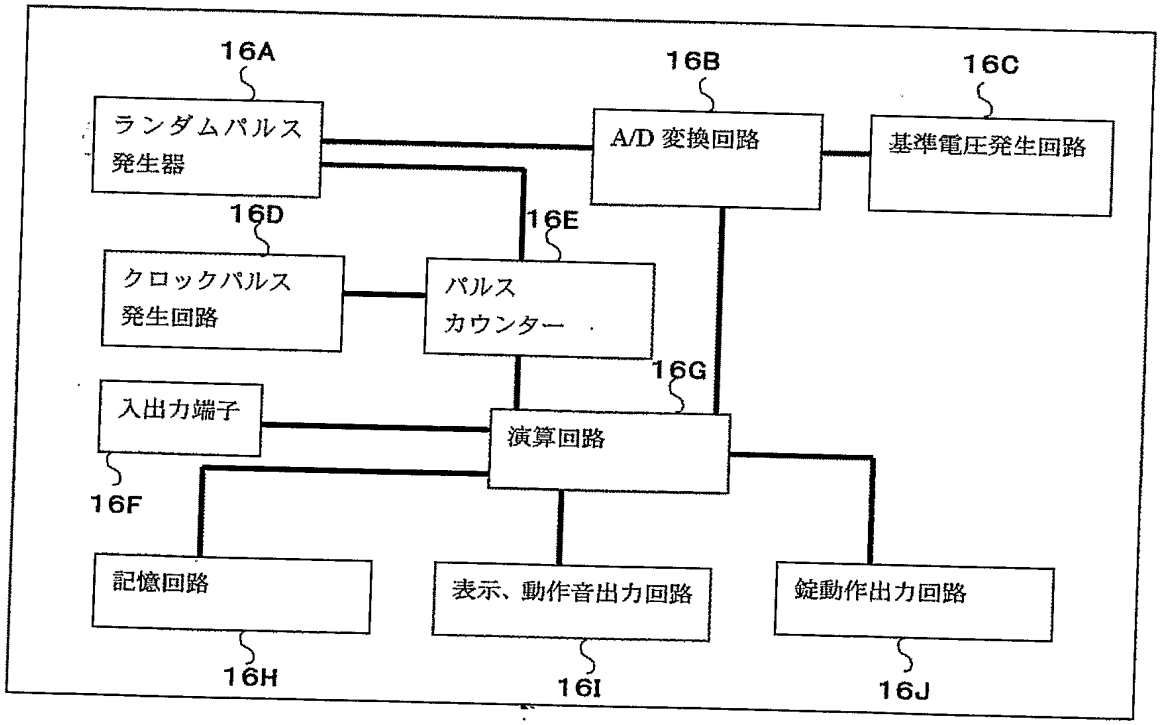
【図８】


鍵本体側
ペアとなる鍵側
(i) 差込検知トリガーモジュールが鍵の挿入を検知すると I(inquire)↓の文字キーを送り、照合データの送信を要求する
(ii) Iコマンドを受信すると保存していた照合データを“R○○・・・○↓”の文字列で鍵本体側に送信する。（○・・・○は、RPGのデータにより変化する）
(iii) 照合データを受信すると、本体側で持っていたデータと比較し、不一致ならNG音を鳴らして終了する。
(iv) 一致なら開錠出力を送信し、開錠する。と同時に最新のRPGのパルスデータ【１００μsec程度のインターバルデータ】を新しい照合データとしてキー側に“W○・・・○↓”コマンドで送信する
(v) Wコマンドを受信すると、新しいデータを次回照合のために保存する。
(vi) Wコマンドで送ったデータが正しくキー側に受け取られたかどうか確認するために再度Iコマンドをキー側に送信する。
(vii) Iコマンドに応答して新しいデータをRコマンドに付随して本体側に返信する。
(viii) 受信データを照合し一致なら成功と判断しOK音を鳴らす。
(ix) 不一致なら再度データをWコマンドでキー側に送信する。以降(v)～(viii)までを何回かリトライしそれでも失敗した場合はFatalError音を鳴らして終える。

【図９】


パルス１
パルス３
電圧
パルス２.
パルス４
クロックパルス

【図１０】


16A
ランダムパルス発生器
16B
A/D 変換回路
16C
基準電圧発生回路
16D
クロックパルス発生回路
16E
パルスカウンター
16G
入出力端子
演算回路
16F
記憶回路
表示、動作音出力回路
錠動作出力回路
16H
16I
16J

16

【書類名】要約書
【要約】
【課題】　本発明は完全なランダムパルスを自発的に発生するランダムパルス発生器を使用して、完全ランダムな信号を認証信号として使用する認証装置及び認証方法を提供する。
【解決手段】　本体、或は相手側、或は本体と相手側の双方に、自発的にランダムパルスを発生するランダムパルス発生器（以下RPGと呼ぶ）と、このＲＰＧが生成するランダムパルスに基づき認証信号を出力する手段と、認証信号を記憶する手段と、認証信号を送信／受信する通信手段と、認証信号の通信制御及び照合等を行う制御手段で構成し、使用者側で完全なセキュリティを確保でき、安全性が確立出来る認証装置を提供する。
【選択図】　図１

# 認定・付加情報

| | |
|---|---|
| 特許出願の番号 | 特願２００４－０５７６２９ |
| 受付番号 | ５０４００３３９９３０ |
| 書類名 | 特許願 |
| 担当官 | 野本　治男　　２４２７ |
| 作成日 | 平成１６年　３月２５日 |

＜認定情報・付加情報＞

【提出日】　平成16年 3月 2日

特願２００４－０５７６２９

# 出願人履歴情報

識別番号　[５９５１２２２６８]

１．変更年月日　１９９５年　７月２４日
[変更理由]　新規登録
住所　千葉県茂原市早野１８２０
氏名　露崎　典平